UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

JACQUELINE MEKHAIL, individually, and on behalf of others similarly situated, Plaintiff, v. NORTH MEMORIAL HEALTH CARE, d/b/a NORTH MEMORIAL HEALTH, Defendant.	Case No. 23-cv-00440 (KMM/TNL) **[PROPOSED] ORDER REGARDING ELECTRONICALLY STORED INFORMATION (ESI) PROTOCOL**

This matter comes before the Court on the Parties' Stipulation for Electronically Stored Information (ESI) Protocol, (ECF No. 72), to expedite the flow of discovery material and to facilitate the prompt resolution of disputes over discovery and electronically stored information. The Court hereby enters an order adopting the Parties' stipulation as follows:

A. General Principles

1. The Parties will conduct discovery in a cooperative, collaborative, and transparent manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions. The Parties will meet and confer about discovery issues in an effort to avoid, resolve, or narrow disputes without court intervention. The Parties, however, do not waive their right to seek court intervention.

2. Parties may obtain all discovery regarding any nonprivileged matter that is relevant to any party's claim or defense, subject to Fed. R. Civ. P. 26(b) and any order by the Court. This shall account for the proportionality standard embodied in Fed. R. Civ. P. 26(b)(1), which requires consideration of the importance of the issues at stake, the amount in controversy, the parties' relative access to relevant information, the parties' resources, and whether the burden or expense of the proposed discovery outweighs its likely benefit. To further the application of the proportionality standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as practicable.

B. Foreign Data Privacy Laws

Nothing in this Stipulation/Order is intended to prevent either party from complying with the requirements of a foreign country's data privacy laws, e.g., the European Union's General Data Protection Regulation (GDPR) (EU) 2016/679. The parties agree to meet and confer before including custodians or data sources subject to such laws in any ESI or other discovery request.

C. ESI Discovery Procedures

1. On-site inspection of electronic media. Such an inspection shall not be required absent a demonstration by the requesting party of specific need and good cause or by agreement of the parties.

2. Search methodology. The parties shall timely confer to attempt to reach agreement on appropriate search terms and queries, file type and date restrictions, data sources (including custodians), and other appropriate computer- or technology-aided

methodologies, before any such effort is undertaken. The parties shall continue to cooperate in an iterative process in negotiating and revising the appropriateness of the search terms and methodology.

a. Prior to running searches:

i. The producing party shall disclose the data sources (including custodians), search terms and queries, any file type and date restrictions, and any other methodology that it proposes to use to locate ESI likely to contain responsive and discoverable information. The parties will work together to compile search terms in an effort to streamline the search process and limit false positives results.

ii. The producing party may provide unique hit counts for each search query in order to provide transparency into the search process. The requesting party is entitled to, within fourteen (14) days of the producing party's unique hit count query disclosure, add up to twenty (20) additional search terms or queries to those disclosed by the producing party absent a showing of good cause or agreement of the parties.

iii. The following provisions apply to search terms/queries of the requesting party. Focused terms and queries should be employed, broad terms or queries, such as product and company names, generally should be avoided. A conjunctive combination of multiple words or phrases (e.g., "computer" and "system") narrows the search and shall count as a single search term. A disjunctive combination of multiple words or phrases (e.g., "computer" or "system") broadens the search, and thus each word or phrase shall count as a separate search term unless they are variants of the same word. The producing party may identify each search term or query returning overbroad results

demonstrating the overbroad results ("false positives" or otherwise overly broad) and a counter proposal correcting the overbroad search or query.

- After production: Within 21 days of the producing party notifying the receiving party that it has substantially completed the production of documents responsive to a request, the responding party may request up to 10 additional search terms or queries.

- Upon reasonable request, a Party shall disclose information relating to network design, the types of databases, database dictionaries, the access control list and security access logs and rights of individuals to access the system and specific files and applications, the ESI document retention policy, organizational chart for information systems personnel, or the backup and systems recovery routines, including, but not limited to, tape rotation and destruction/overwrite policy.

- If after the parties have identified initial document custodians, and the requesting party believes that additional document custodians or sources should be added after reviewing the produced documents, then the requesting party shall advise the producing party in writing of the proposed additional document custodians or sources of data and the basis for such request.

If a dispute arises related to Section 2 (or any other provision of this Stipulation), the parties will meet and confer in good faith in an effort to resolve or narrow the dispute in accordance with Local Rule 7.1. If the parties are unable to fully resolve the dispute, the matter may be brought to the Court.

3. Format.

a. ESI will be produced to the requesting party with searchable text where reasonably available using Optical Character Recognition ("OCR") technology, in an agreeable standard format to be decided between parties. Except for where indicated or specifically requested by counsel, the default format for production of all ESI shall be single-page TIFF files with extracted text, if available, and corresponding metadata in a load file in compliance with Section 6 below. Acceptable formats include, but are not limited to, native files, multi-page TIFFs (with a companion OCR or extracted text file), single-page TIFFs (only with load files for e-discovery software that includes metadata fields identifying natural document breaks and also includes companion OCR and/or extracted text files), and searchable PDF.

b. Unless otherwise agreed to by the parties, files that are not easily converted to image format, such as spreadsheet (*e.g.*, XML), Power Point, database, and drawing files (*e.g.,* CAD), will be produced in native format or near-native format with a TIFF image placeholder. An exception will be made for files that contain privileged information. The producing party shall have the options of producing these files in a redacted image format or, if the parties agree, as a modified native file. Native and near-native files shall be named to match the endorsed bates number on the corresponding TIFF image placeholder page (e.g., ABC000001.xls)

i. For the purposes of this subsection, "near-native format" means the format of ESI that preserves the functionality, searchability, and integrity of a native format item when it is unreasonable or unduly burdensome to produce the item in

native format, including where redactions to an otherwise native format item are made. For example, an Excel spreadsheet is a suitable near-native format for production of Google Sheets. If particular documents warrant a different format, the parties will cooperate to arrange for the mutually acceptable production of such documents.

c. Each document image file shall be named with a unique number (Bates Number). File names should not be more than twenty characters long or contain spaces. Bates numbers shall be sequential padded, alphanumeric (e.g., ABC000001) and contain no spaces or dashes between the production prefix (ABC) and the padded production number (000001). When a text-searchable image file is produced, the producing party must preserve the integrity of the underlying ESI, i.e., the original formatting, the metadata (as noted below) and, where applicable, the revision history.

d. If a document is more than one page, the unitization of the document and any attachments and/or affixed notes (full families) shall be maintained as they existed in the original document.

e. The parties shall produce their information in the following format: single-page images and associated multi-page text files containing extracted text where reasonably available using OCR technology or with appropriate software load files containing all information required by the litigation support system used by the receiving party. If implementing a third-party ESI vendor, party's vendors are encouraged to communicate prior to production to ensure delivery specs are acceptable for the review software.

f. The full text of each electronic document shall be extracted ("Extracted Text") and produced in text file where reasonably available using OCR technology. The Extracted Text shall be provided in searchable ASCII text format (or Unicode text format if the text is in a foreign language) and shall be named with a unique Bates Number (e.g., the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension).

g. Production images shall be endorsed with their Bates Number and appropriate protective declarations.

4. Document Families. Entire document families must be produced, even if only part of the document family is responsive. This does not require producing parts of a document family that may be withheld due to privilege or another applicable basis.

5. De-duplication. The parties may de-duplicate their ESI production across custodial and non-custodial data sources after disclosure to the requesting party, and the deduplicate custodian information removed during the de-duplication process shall be tracked in a duplicate/other custodian field in the database load file.

a. De-duplication shall be performed only at the parent document level so that the attachments are not de-duplicated against identical stand-alone versions of such documents and vice versa (*e.g.*, a standalone document that is also an attachment to an email should not be deduplicated);

b. Attachments to emails or other documents shall not be disassociated from the parent email or document, even if they are exact duplicates of another Document in the production; and

c. The remaining version of the document after de-duplication will contain a list of all custodians and file paths from all of the duplicates not produced.

6. Email Threading. The parties may use analytics technology to identify email threads and need only produce the unique most inclusive copy and related family members and may exclude less inclusive email strings. Email thread suppression shall not eliminate the ability of the receiving party to identify every custodian who had a copy of the produced document or email, and the producing party will not remove from production any unique branches and/or attachments contained within an email thread.

7. Metadata fields. The parties agree that the following metadata fields should be produced, and only to the extent it is reasonably accessible and non-privileged: (i) document type; (ii) custodian and duplicate custodians (or storage location if no custodian); (iii) author/from; (iv) recipient/to, cc and bcc; (v) title/subject; (vi) email subject; (vii) file name; (viii) file size; (ix) file extension; (x) original file path; (xi) date and time created, (xii) sent, modified and/or received; (xiii) hash value; (xiv) document type; and (xv) email thread index. The list of metadata type is intended to be flexible and may be modified by further written agreement of the parties. Where reasonably available, such metadata and confidential designation information shall be provided in a delimited file for any production documents with the following identifiers:

1) BegProd	Beginning Production # (all documents)
2) EndProd	Ending Production # (all documents)
3) BegAttach	Beginning Attachment # (all documents)
4) EndAttach	Ending Attachment # (all documents)
5) ParentID	Parent Production # (all documents)

6) ProtectiveDeclaration	Confidentiality Designation (all documents)
7) PageCount	Page Count (all documents)
8) Custodian	Custodian (all documents)
9) AllCustodians	Primary and all duplicate custodians (all documents)
10) Author	Author (electronic documents)
11) DateModified	Last Modified Date (electronic documents)
12) TimeModified	Last Modified Time (electronic documents)
13) DateReceived	Received Date (email documents)
14) DateSent	Sent Date (email documents)
15) FileExtension	File Extension (email and electronic documents)
16) EmailSubject	Email Subject (email documents)
17) FileName	Filename (electronic documents)
18) FileSize	Filesize (email and electronic documents)
19) FilePath	Folder/path (email and electronic documents)
20) MD5Hash	MD5 Hash Value (email and electronic documents)
21) People – BCC	BCC (email documents)
22) People – CC	CC (email documents)
23) People – From	From (email documents)
24) People – To	To (email documents)
25) TimeReceived	Received Time (email documents)
26) TimeSent	Sent Time (email documents)
27) Title	Title (electronic documents)
28) NativePath	Native File Path (email and electronic documents)
29) TextPath	Text File Path (all documents)

8. Hard-Copy Documents. If the parties elect to produce hard-copy documents in an electronic format, the production of hard-copy documents will include a cross-

reference file that indicates document breaks and sets forth the custodian or custodian/location associated with each produced document. Hard-copy documents will be scanned using Optical Character Recognition (OCR) technology and searchable ASCII text files will be produced (or Unicode text format if the text is in a foreign language), unless the producing party can show that the cost would outweigh the usefulness of scanning (for example, when the condition of the paper is not conducive to scanning and will not result in accurate or reasonably useable/searchable ESI). Each file will be named with a unique Bates Number (e.g., the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension).

9. Exception Reporting. If any documents not otherwise identified as system or operating files, the producing party must disclose processing exceptions that are unresolved, such as documents that cannot be opened due to encryption or other processing issues.

D. Preservation of ESI

The parties acknowledge that they have a common law obligation, as expressed in Federal Rules of Civil Procedure, Rule 37(e), to take reasonable and proportional steps to preserve discoverable information in the party's possession, custody, or control. With respect to preservation of ESI, the parties agree as follows:

1. Absent a showing of good cause by the requesting party, the parties shall not be required to modify the procedures used by them in the ordinary course of business to back-up and archive data; provided, however, that the parties shall preserve all discoverable ESI in their possession, custody, or control.

2. The parties will supplement their disclosures in accordance with Federal Rules of Civil Procedure, Rule 26(c) with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made (unless excluded under Section (D)(3)).

3. Absent a showing of good cause by the requesting party, the following categories of ESI need not be preserved:

a. Deleted, slack, fragmented, or other data only accessible by forensics.

b. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

c. On-line browser access data such as temporary internet files, history, cache, cookies, and similar files.

d. Data in metadata fields that are frequently updated automatically, such as last-opened dates (see also Section (E)(6)).

e. Back-up data that are duplicative of data that are more accessible elsewhere.

f. Server, system, or network logs.

g. Data remaining from systems no longer in use that is unintelligible on the systems used.

h. Electronic data (*e.g.*, email, calendars, contact data, and notes) sent to or from mobile devices (e.g., iPhone, iPad, Android devices), provided that a copy of all such electronic data is automatically saved elsewhere (such as a server, laptop, desktop computer, or "cloud" storage).

E. Privilege

1. A producing party shall create a privilege log of all documents fully withheld from production on the basis of a privilege or protection, unless otherwise agreed or accepted by this Stipulation and Order. Privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged, work-product protection, or any other applicable privilege). For ESI, the privilege log may be generated using available metadata, including author/recipient or to/from/cc/bcc names; the subject matter or title; and date created/sent/received. A party must manually populate its privilege log fields where the required information is not provided by the objective metadata.

a. Privilege logs will be produced to all other parties no later than 30 days after delivering a production, unless a different deadline is agreed to by the parties.

b. The privilege log shall identify for each claimed privileged document: (i) a unique document identifier, (ii) a description sufficient to allow the Parties to analyze the relevance and claimed privilege; (iii) the date of the document; (iv) author of the document; (v) all recipients of the document; (vi) date sent; (vii) date received; and (viii) the claimed basis for withholding the document.

2. Redactions need not be logged so long as the basis for the redaction is clear on the face of the redacted document.

3. With respect to privileged or work-product information generated after the filing of the complaint, parties are not required to include any such information in privilege logs after February 22, 2023.

4. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Federal Rules of Civil Procedure, Rule 26(b)(3)(A) and (B).

5. Pursuant to Federal Rules of Evidence 502, the production of any documents in this proceeding shall not, for the purposes of this proceeding or any other federal or state proceeding, constitute a waiver by the producing party of any privilege applicable to those documents, including the attorney-client privilege, attorney work-product protection, or any other privilege or protection recognized by law. Information produced in discovery that is protected as privileged or work product shall be immediately returned to the producing party after the receiving party is notified and the producing party has shown that it has taken reasonable steps to avoid inadvertent disclosures. Inadvertent privileged production of documents shall not constitute a waiver of such protection.

Dated: _____, 2024

TONY N. LEUNG
United States Magistrate Judge
District of Minnesota